Certificate of Cloud Security Knowledge (CCSK)

The Certificate of Cloud Security Knowledge (CCSK) provides evidence that an individual has successfully completed an examination covering the key concepts of the CSA guidance and ENISA whitepaper.

The Cloud Security Alliance has developed a widely adopted catalogue of security best practices, the "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1". In addition, the European Network and Information Security Agency (ENISA) whitepaper "Cloud Computing: Benefits, Risks and Recommendations for Information Security" is an important contribution to the cloud security body of knowledge.

The Certificate of Cloud Security Knowledge (CCSK) provides evidence that an individual has successfully completed an examination covering the key concepts of the CSA guidance and ENISA whitepaper.

Cloud Security Alliance - Security Guide for Critical Areas of Focus in Cloud computing V2.1

European Network and Information Security Agency (ENISA) – Cloud Computing: Benefits, Risks and Recommendations for Information Security

1. Security benefits of cloud computing

- Security and the benefits of scale
- Security as a market differentiator
- Standardised interfaces for managed security services
- Rapid, smart scaling of resources
- Audit and evidence-gathering
- More timely and effective and efficient updates and defaults

- Audit and SLAs force better risk management
- Benefits of resource concentration

2. Risk assessment

- Use-case scenarios
- Risk assessment process

3. Risks

Policy and organizational risks

- R.1 Lock-in
- R.2 Loss of governance
- R.3 Compliance challenges
- R.4 Loss of business reputation due to co-tenant activities
- R.5 Cloud service termination or failure
- R.6 Cloud provider acquisition
- R.7 Supply chain failure

Technical risks

- R.8 Resource exhaustion (under or over provisioning)
- R.9 Isolation failure
- R.10 Cloud provider malicious insider - abuse of high privilege roles
- R.11 Management interface compromise (manipulation, availability of infrastructure)
- R.12 Intercepting data in transit
- R.13 Data leakage on up/download, intra-cloud
- R.14 Insecure or ineffective deletion of data
- R.15 Distributed denial of service (DDoS)
- R.16 Economic denial of service (EDOS)
- R.17 Loss of encryption keys
- R.18 Undertaking malicious probes or scans
- R.19 Compromise service engine
- R.20 Conflicts between customer hardening procedures and cloud environment

Legal risks

- R.21 Subpoena and e-discovery
- R.22 Risk from changes of jurisdiction
- R.23 Data protection risks
- R.24 Licensing risks

Risks not specific to the cloud

- R.25 Network breaks
- R.26 Network management (ie, network congestion / mis-connection / non-optimal use)
- R.27 Modifying network traffic
- R.28 Privilege escalation
- R.29 Social engineering attacks (ie, impersonation)
- R.30 Loss or compromise of operational logs
- R.31 Loss or compromise of security logs (manipulation of forensic investigation)
- R.32 Backups lost, stolen
- R.33 Unauthorized access to premises (including physical access to machines and other facilities)
- R.34 Theft of computer equipment

- R.35 Natural disasters

4. Vulnerabilities

- Vulnerabilities not specific to the cloud

5. Assets

6. Recommendations and key messages

- Information assurance framework
- Introduction
- Division of liabilities
- Division of responsibilities
- Software as a Service
- Platform as a Service
- Infrastructure as a Service
- Methodology
- Note of caution
- Note to governments
- Information assurance requirements
- Personnel security
- Supply-chain assurance
- Operational security
- Identity and access management
- Asset management
- Data and Services Portability
- Business Continuity Management
- Physical security
- Environmental controls
- Legal requirements
- Legal recommendations
- Legal recommendations to the European Commission
- Research recommendations
- Building trust in the cloud
- Data protection in large-scale cross-organizational systems
- Large-scale computer systems engineering (systems)